

UNITED STATES DISTRICT COURT

for the  
Western District of Arkansas  
Fayetteville Division

US DISTRICT COURT  
WESTERN DISTRICT OF ARKANSAS  
FILED

APR 17 2017

DOUGLAS F. YOUNG, Clerk  
By  
Deputy Clerk

In the Matter of the Search of )  
**Bitcoin Wallets:** )  
- 1KXhP8nUtNzjKFGQQXDFubhMQ8LfVdKJ2Y )  
- NFAUpuGFa2HHygsHTsYZp7rLki89VZb5ye )  
- MyJFDbxQbNh6jUJVwX9yJL2kaAfcdbd9uwr )  
- 42DpM2KjD2HVVAqLqsNpJ2AF9fiw72x9j )  
GEHZA7DtXMYjUgqMYg6D3WbwaVe4vU )  
MveKAzAiA4j8xgUi29TpKXpm3y9FQS2 )  
- 17F5rCCPArYwg4pN4amA4naG99D3cCu6F7 )

Case Number; 5-17-cm-36

All from digital devices owned and maintained by Peng CHANTHALANGSY

APPLICATION FOR A SEARCH AND SEIZURE WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search and seizure warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Western District of Arkansas (*identify the person or describe property to be searched and give its location*):

**SEE ATTACHMENT A**

The person or property to be searched and seized, described above, is believed to conceal (*identify the person or describe the property to be seized*): **Bitcoin--SEE ATTACHMENT B**

The basis for the search and seizure under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ X evidence of a crime;  
☐ X contraband, fruits of crime, or other items illegally possessed;  
☐ X property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search and seizure is related to a violation of **18 U.S.C. § 2251/2252 and 21 U.S.C. § 841**, and the application is based on these facts:

☒ X Continued on the attached sheet—Attachment C.

Sworn to before me and signed in my presence.

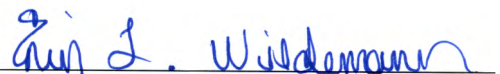
Date: 4/17/17

City and state: FAYETTEVILLE AR



Applicant's signature

Gerald F. Faulkner, HSI SPECIAL AGENT



Judge's signature

ERIN WIEDEMANN, US MAGISTRATE JUDGE

Printed name and title

**ATTACHMENT A**

**DESCRIPTION OF PROPERTY TO BE SEARCHED AND SEIZED**

Bitcoin wallet numbers:

- 1KXhP8nUtNzjKFGQQXDFubhMQ8LfVdKJ2Y
- NFAUpuGFa2HHygsHTsYZp7rLki89VZb5ye
- MyJFDbxQbNh6jUJVwX9yJL2kaAfcdb9uwr
- 42DpM2KjD2HVVAqLqsNpJ2AF9fiw72x9jGEHZA7DtXMYjUgqMYg6D3WbwaVe4vUMveKAzAiA4j8xg  
Ui29TpKXpm3y9FQS2
- 17F5rCCPArYwg4pN4amA4naG99D3cCu6F7

All from digital devices owned and maintained by Peng CHANTHALANGSY

## ATTACHMENT B

### DESCRIPTION OF ITEMS TO BE SEARCHED AND SEIZED

1. Any and all hidden services accounts<sup>1</sup> used in furtherance of the offenses described above, including, but not limited to, Dark Web / Darknet market accounts, associated Dark Web / Darknet forum accounts and Tor-based email accounts.
2. Any and all peer to peer (P2P) virtual currency trading platform accounts, with no legitimate or identified service provider to which legal process may be served, used in furtherance of the offenses described above, including, but not limited to, localbitcoins.com<sup>2</sup> accounts or bitcoin-otc internet relay chat channel<sup>3</sup> accounts.
3. Virtual currency in any format, including but not limited to, wallets (digital and paper), public keys (addresses), bitcoin, bitcoin miners, crypto-currency, and private keys.

---

<sup>1</sup> Hidden services (.onion services) are accessed through the Tor anonymity network. Most are considered dark web services with no legitimate or identified service provider to which legal process may be served.

<sup>2</sup> LocalBitcoins, OY (and their associated web platform, localbitcoins.com “LBC”) is a Finnish company which is not a licensed money transmitting business registered with the U.S. Government and compliant with the Bank Secrecy Act, which requires establishment and maintenance of anti-money laundering (AML) programs in accordance with know your customer (KYC) rules, such as identifying persons involved in currency transactions over certain thresholds. LBC is not considered a legitimate service provider to which legal process may be served for accurate subscriber information or account seizure.

<sup>3</sup> Internet Relay Chat (IRC) is a decentralized chat system which enables people with an installed client (computer program which sends and receives messages to and from an IRC server via the internet) to join in live discussions with anyone else connected in the same manner. The IRC server ensures that all messages are broadcast to everyone participating in a discussion. There can be many discussions going on at once; each one is assigned a unique channel. One such channel is #bitcoin-otc, in which virtual currency trades are negotiated and arranged. All transactions that may occur are conducted directly between counterparties, without any participation or intermediation from the hosts of IRC servers, and therefore no entity to which legal process may be served for accurate subscriber information, transactional history or account seizure.

ATTACHMENT C

UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF ARKANSAS

STATE OF ARKANSAS

:  
:  
:  
:  
:

ss. AFFIDAVIT

COUNTY OF WASHINGTON

Affidavit in Support of Application for Search and Seizure Warrant

I, Gerald Faulkner, being duly sworn, depose and state as follows:

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations (“HSI”), currently assigned to the Assistant Special Agent in Charge Office in Fayetteville, Arkansas. I have been so employed with HSI since April, 2009. As part of my daily duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, online enticement, transportation, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2251A, 2422(b), 2252(a) and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also participated in the execution of numerous search warrants and arrest warrants, a number of which involved child exploitation and/or child pornography offenses. This affidavit is being submitted based on information from my own investigative efforts as well as information obtained from others who have investigated this matter and/or have personal knowledge of the facts herein.

**Purpose of Affidavit**

2. Your Affiant respectfully submits there exists probable cause that the SUBJECT ACCOUNTS contain digital currency used to facilitate the purchase or sale of illegal narcotics/child pornography, or instrumentalities of such, involved in violations of Title 18, United States Code, Sections 2252/2252A (Trafficking and Possession of Child Pornography) and Title 21, United States Code, Sections 841 (Distribution of a Controlled Substance).

described as:

a. Bitcoin digital currency wallets owned and maintained by Peng

CHANTHALANGSY, identified by Bitcoin wallet numbers:

- 1KXhP8nUtNzjKFGQQXDFubhMQ8LfVdKJ2Y
- NFAUpuGFa2HHygsHTsYZp7rLki89VZb5ye
- MyJFDbxQbNh6jUJVwX9yJL2kaAfcdb9uwr
- 42DpM2KJjD2HVVAqLqsNpJ2AF9fiw72x9jGEHZA7DtXMYjUgqMYg6D3WbwaVe4vU  
MveKAzAiA4j8xgUi29TpKXpm3y9FQS2
- 17F5rCCPArYwg4pN4amA4naG99D3cCu6F7

(herein after referred to as **SUBJECT ACCOUNTS**) described in Attachment A of these Applications in addition constitute evidence, fruits and instrumentalities of violations of Title 18, United States Code, Sections 2251 and 2252 *AND* Title 21, United States Code, Sections 841. As such, it does not include all of the information known to me as part of this investigation, but only information sufficient to establish probable cause for the requested search warrant and seizure warrant.

**Statutory Authority**

3. This investigation concerns alleged violations of **Title 18, United States Code, Sections 2251 and 2252, relating to Child Pornography AND Distribution of a Controlled Substance, Methamphetamine in violation of Title 21, United States Code, Sections 841.**

a. Under 18 U.S.C. 2251 and 2252, it is a federal crime to Receive, Distribute, Possess, or Access a device with the Intent to view Child Pornography as that term is defined by federal law

i. The term “minor,” as used herein, is defined pursuant to Title 18, United States Code, Section 2256(1) as “any person under the age of eighteen years.” The term Child Pornography, as used in this affidavit herein, is defined in Title 18, United States Code, Section 2256(8), to include the use of a minor engaged in sexually explicit conduct. Sexually explicit conduct is likewise defined in Section 2256(2), to include sexual intercourse, oral and anal sex, masturbation, and lascivious exhibition of the genitals.

b. **Title 21, United States Code, Sections 841**, it is a federal crime to distribute, sale, or exchange for value any controlled substance, including Methamphetamine.

4. There is also probable cause to believe that property contained in the SUBJECT ACCOUNTS are **subject to seizure and forfeiture**:

- Pursuant to Title 18, United States 18 U.S.C. § 2253, upon conviction of an offense listed in violation of 18 United States Code, Section 2252/2252A

(collectively “Child Pornography” offenses), the defendant shall forfeit any property, real or personal, used or intended to be used to commit or to promote the commission of the offenses .

- Pursuant to Title 21, United States Code, Section 853, upon conviction of an offense in violation of Title 21, United States Code, Sections 841, 846, and 856 the defendants, shall forfeit to the United States of America any property constituting, or derived from, any proceeds obtained, directly or indirectly, as the result of such offense[s] and any property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, the offense(s).
- IT is the intent of the United States, pursuant to Title 18 U.S.C. § 2253(b), incorporating by reference Title 21 U.S.C. § 853 to seek forfeiture of any other property of said defendants up to the value of the above forfeitable property.

#### **SURFACE WEB – DEEP WEB – DARK WEB / DARKNET**

5. The Surface Web is defined as a collection of hyperlinks that are indexed by search engines. These search engines, such as “Google”, allow users access to website pages/content that are accessible through the Surface Web and is most commonly used by most individuals accessing the Internet without the use of any special programs or networks.

6. The Dark Web / Darknet and the Deep Web consist of website pages and data that are beyond the reach of Surface Web search engines. Some of what makes up the Deep Web /

Darknet is comprised of abandoned, inactive web pages, but the majority of data that lies within have been crafted to deliberately avoid detection in order to be utilized anonymously.

SURFACE WEB	DEEP WEB	DARK WEB / DARKNET
Anything that can be found via a typical search engine (Google Chrome, Safari, etc.)	Things your typical search engine can't find (government databases, libraries, etc.)	A small portion of the Deep Web that is intentionally hidden and made inaccessible via search engines (the Tor network, only accessible via Tor browser)

7. The Dark Web / Darknet is an overlay network that can only be accessed with specific software, configurations, or authorizations, often using non-standard communication protocols and ports. Two typical Dark Web / Darknet types are peer-to-peer networks (usually for file sharing) and privacy networks such as TOR.

### **TOR ("The Onion Router")**

8. TOR stands for "The Onion Router" which is a network typically decentralized, routing traffic through a wide-spread system of servers, which are often provided by volunteers. The complex routing system makes it difficult to trace communications. Normally, when accessing the Surface Web, a computer directly accesses the server hosting the website a user is visiting. In a TOR network, this direct link is broken, and the data is instead bounced around a number of intermediaries before reaching its destination. The communication registers on the network, but the transport medium is prevented from knowing who is doing the communication. TOR makes a popular "Onion Router" that is fairly user-friendly for anonymous communication and accessible to most computer operating systems. TOR directs Internet traffic through a free,



worldwide, volunteer network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using TOR makes it more difficult for Internet activity to be traced back to the user, this includes: visits to websites, online posts, instant messages and other communication forms. TOR's use is intended to protect the personal privacy of users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored.

9. The TOR network can also be used to search the Surface Web anonymously. It also allows users to visit websites published anonymously on the TOR network, which are inaccessible to users not using TOR. This is one of the largest and most popular sections of the Dark Web / Darknet.

10. TOR websites addresses do not look like ordinary URLs. They are composed of a random-looking string of characters followed by ".onion". An example of a hidden website address on the TOR network is listed as being <http://dppmfxaacucguzpc.onion/>. This example website will take a user to a directory of Dark Web / Darknet websites if the user has TOR installed on their operating system. If the user does not have TOR installed then it is completely inaccessible.

11. ".onion" sites are a Top Level Domain (TLD) host suffix designating an anonymous hidden service reachable through the TOR network. Such addresses are not actual Domain Name Server (DNS) names, and the ".onion" TLD is not in the Internet DNS root, but with the appropriate proxy software installed (TOR), Internet programs such as web browsers can access sites with ".onion" addresses by sending the request through the TOR network. The purpose of using such a system is to make both the information provider and the person

accessing the information more difficult to trace, whether by one another, by an intermediate network host, or by an outsider.

12. To access “.onion” sites, users follow these steps utilizing non-specific electronic devices such as a desktop computer, laptop, tablet, etc.:

- Navigate to the TOR website through the Surface Web
- Download the TOR browser bundle and install just like any other computer software program
- Start the TOR browser at which time the user will be connected to the TOR network

13. One of the purposes of the Dark Web / Darknet is to provide a venue for private communication when public communication is undesirable, dangerous or not permitted. Special-purpose Dark Web / Darknet websites are most commonly used for illegal file sharing, which includes copyrighted media, pirated software, malware programs and child pornography as well as marketplaces for the sale and distribution of illegal narcotics.

### **CRYPTOCURRENCY (BITCOIN)**

14. Bitcoin is a digital currency that is stored on Bitcoin addresses sitting in Bitcoin wallets. All transactions moving Bitcoins from one address to another have to be electronically signed and then are propagated to the Bitcoin network. The peer-to-peer nature of the network does not mean that the knowledge about the transaction is limited to two parties — sender and the receiver. On the contrary, all transactions are propagated across the whole Bitcoin network to make sure every single participant hears about them.

15. Each of the participants keeps a log of all incoming and outgoing transactions. However, due to network latency and other reasons, different users may keep track of different sets of transactions at any moment.

16. Bitcoin is based on a combination of several technologies, one of which is a public key cryptography dictating that two different keys are required to send and receive

transactions. A public key can be distributed to anyone in order to receive a payment while the private key that should only be known to its owner is used to create a signature for a transaction that cannot be forged. Public key cryptography solves two fundamental problems all digital currencies face: 1) It allows user to uniquely identify their addresses in the system and 2) It prevents users to spend coins they do not own.

17. Both the private and public keys are stored in a Bitcoin wallet. One person can possess any number of Bitcoin wallets and each wallet can store any number of private keys. These private keys are used to generate public keys. A public key, when hashed, turns into a Bitcoin address. Bitcoin addresses can be — with a bit of simplification — thought of as bank accounts or email addresses as they can be publicly shown to anyone to receive payments. However, unlike bank accounts or email addresses, which keep their content private, knowledge of the Bitcoin address reveals Bitcoin balance and transactions sent to and from this address. A private key acts as a lock for the Bitcoin addresses. The owner of a private key has access to the funds stored on the corresponding bitcoin address. This means that the owner can move funds from his address to any other address of his choice. It is not possible to derive a private key from a Bitcoin address and therefore it is absolutely safe to share the Bitcoin address.

18. In addition, there are three most common representations of the public key or a Bitcoin address. A public key is rarely found; what is usually discovered on paper or in electronic form is a Bitcoin address:

**1. Public key:**

*04e2ff72520d37d88c61d0bac1caa6fcec4ffefd372d22247686affa1ebdeea52d0dd2135  
4ed98d2173abee0977ce4c62648290fb34fe172f0153b98bf132fc66*

**2. Normal Bitcoin address:** *13mE8VYvGym8Rj9ddHoagcNxmDs1SaxbNJ*

3. **Pay-to-script hash Bitcoin address:** *3KgtbGgaX2ngstNpvyv7LwpHSweVeqGbpM*

### **BITCOIN AND THE DARK WEB / DARKNET**

19. Bitcoin is well established within the Dark Web / Darknet and has gradually become a currency of choice for all sorts of criminal-to-criminal payments. While other cryptocurrencies such as Litecoin, Dash or Monero have been accepted by some of the marketplaces, the overwhelming majority of trade is still facilitated by Bitcoin. Commonly traded, sold or purchased items on the Dark Web / Darknet include illegal narcotics, fake IDs, counterfeit currency, compromised data including payment cards or accounts at online services, malware kits, weapons, explosives and chemical substances.

20. Although most users of the Dark Web/ Darknet do not exchange child pornography for monetary gain, commercial exploitation has been observed by law enforcement. This may be in the form of a Bitcoin payment for access to pay sites for either live streaming of child abuse or child pornography/exploitation images. More inventive approaches include securing Bitcoin payments for crowdfunding Dark Web / Darknet websites, where offenders ask for financial contribution to facilitate their access to minor victims, such as covering travel expenses to the third world countries, in exchange for privileged access to a newly acquired minor victim for a sexual encounter.

### **BITCOIN MINING**

21. Unlike traditional currency, Bitcoin exists outside of national control. Ownership of Bitcoin can be gained in three primary ways: 1) users can buy them 2) users can get paid in them in return for a product or service 3) users can make them through a process called Bitcoin mining. Bitcoin mining is so called because it resembles the mining of other commodities: it

requires exertion and it slowly makes new currency available at a rate that resembles the rate at which commodities like gold are mined from the ground.

22. Bitcoin mining is the mechanism used to introduce Bitcoins into the system: miners are paid any transaction fees as well as a subsidy of newly created coins. This both serves the purpose of disseminating new Bitcoins in a decentralized manner as well as motivating people to provide security for the system. The Bitcoin system is set up to limit the total number of Bitcoins that will ever be available in the world pool. That limit in total availability artificially forces value on each coin because the resource is designed to have scarcity.

23. Bitcoins come into existence as the result of increasingly complex calculations that incur both computing hardware and energy cost. The Bitcoin system requires that each new Bitcoin is incrementally harder to “mine” than the preceding coin. This means that each new Bitcoin requires more and more calculation power than the coins that came before. Given that Bitcoin mining is designed to always need more computing power, a market was developed for custom Bitcoin mining computers, machines built with custom Application Specific Semiconductor (ASIC) chips designed to optimize the processing of the Bitcoin mining algorithms. A Bitmain Antminer is a machine specifically sold with ASIC chips to enable users to “mine” Bitcoins. Each coin has a cost production, the profit attributable to each coin, therefore, can be calculated as the net selling price of the coin, minus the cost to produce. Bitcoin mining profitability is all about getting the hash rate (speed of calculation) high enough, while the cost of hardware and energy is low enough.

### **PROBABLE CAUSE**

24. Between January 2017 and March 2017, officers with the Rogers Police Department, located in Benton County Arkansas, conducted numerous undercover purchases of both Methamphetamine and Marijuana from a Target identified as Peng CHANTHALANGSY. During said time period, an informant working for Rogers Police Department purchased a usable amount of methamphetamine from CHANTHALANGSY from on three separate occasions in exchange for a total of \$220 dollars of undercover drug buy money. Moreover, Rogers Police were able to purchase marijuana from CHANTHALANGSY on 2 separate occasions in exchange for a total of \$120 of covert drug buy money. Based on the above-described undercover purchases, on Monday March 13, 2017, an Arkansas state search warrant was applied for and obtained for the residence of Peng CHANTHALANGSY located at 4007 West Olive Street in Rogers, Arkansas. The residence was suspected of containing evidence of possession of a controlled substance with the intent to deliver (Methamphetamine) and possession of drug paraphernalia. Drug Task Force Officers (TFO) had previously conducted two controlled transactions with CHANTHALANGSY, with the most recent being on March 13<sup>th</sup>, 2017, involving the controlled purchase of 10 grams of methamphetamine. The State authorized search warrant allowed for the confiscation of, among other things, digital devices capable of containing evidence of drug transactions.

25. At approximately 1859 hours, a knock and announce search warrant for the residence located at 4007 West Olive Street, Rogers, Arkansas was executed. Of note, law enforcement spoke with CHANTHALANGSY's adult nephew who stated CHANTHALANGSY made money from mining Bitcoin. During the search, law enforcement located approximately 131 grams (4.62oz) of marijuana, approximately 43.9 grams (1.6oz) of methamphetamine, approximately 1.2 grams of cocaine, and \$17,320 in U.S. Currency (including \$3,200 in

previously recorded drug buy money). While searching the garage of the residence law enforcement also located six operating “Bitmain Antminers” set up and organized on white plastic crates and each miner was connected to a separate 1300 watt power supply. It should be noted that the miners were connected directly to each other through a series of wired system links. Each miner was also connected to a 16 port desktop switch/router via Ethernet cable. The desktop switch/router appeared to be connected to the cable or internet access line of the residence. It was discovered that the set-up is commonly referred to as a Bitcoin mine, which are processors that confirm or deny internet transactions that use the virtual currency Bitcoin. For every transaction the processors confirm the owner/user of the “Antminers” accrue, a certain amount of Bitcoin can be used to purchase physical items over the internet or sold/traded for U.S. Currency. Multiple “Antminers” that were operating in the garage had an address label attached to them that displayed “Chanthalangsy, Peng 4007 W Olive St Rogers, AR 72756”. Law enforcement also located a black Cyborg iBuyPower I-Series 901 computer in CHANTHALANGSY’s bedroom. Consequently, all digital devices were seized pursuant to the search warrant, as possibly containing evidence of drug transactions.

26. On Thursday, March 16, 2017, TFO Dennis Schumacher, a digital forensic examiner with HSI, began examining the digital storage devices confiscated from the West Olive Street address for evidence pertaining to the sale, purchasing, and distribution of drugs. During the examination, it was noted that the iBuyPower CyborgX computer contained two hard drives, one was Kingston 120GB Solid State drive and the other was a Hitachi 1TB hard drive. The Hitachi 1TB Hard Drive was imaged on March 17, 2017 and the Kingston 120GB Solid State drive was imaged March 20, 2017. During this process, the examiner noted that the device(s) contained relevant information pertaining to the drug case. However, of significance to the

current warrant request, the examiner located on the Hitachi 1TB hard drive several images of child pornography along with multiple child erotica images. Consequently, the examiner stopped the review of the seized items in order to obtain a federal search warrant allowing for the search for child pornography. One of the particular images the examiner viewed prior to stopping his examination was described as a 3 to 4 years old completely nude female standing with one leg on a stool and the other leg extended up to what appears to be a counter. Per TFO Schumacher, the pose of the minor depicted in the image was provocative, in that the focal point of the image is of the minor's genital area. The title of the image is "Russian Lolitas. Professional Series", [www.loliaspro.com](http://www.loliaspro.com).

27. On March 23, 2017, based on the child pornography image located on CHANTHALANGSY's seized device, your Affiant applied for and received a federal search warrant for possible violations of 18 U.S.C. 2251 and 2252.

28. On March 24, 2017, after receipt of the newly acquired federal search warrant, TFO Schumacher resumed his forensic examinations on CHANTHALANGSY's iBuyPower CyborgX computer containing the two hard drives, Kingston 120GB Solid State drive and Hitachi 1TB hard drive. TFO Schumacher went back to the location where he had seen the child pornography images on the Hitachi 1TB hard drive, "\\here\\New folder\\". While looking through a few of the files, TFO Schumacher found several images of child pornography. These images consisted of pictures and videos with children between three (3) and twelve (12) years of age.

29. On March 27, 2017, TFO Schumacher provided your Affiant with a copy of a disk containing approximately one-hundred (100) images of suspected child pornography obtained from CHANTHALANGSY's Hitachi 1TB hard drive. Your Affiant reviewed the images and videos and confirmed them to be child pornography.



30. Three (3) of the videos of child pornography reviewed are described as being:

a. Video: "5yo anal and vaginal"

Length: :46

Description: This video depicts a prepubescent minor female approximately four (4) to six (6) years of age lying on a bed completely naked with an adult male's erect penis penetrating her vagina and anus.

b. Video: "Pthc k4 – 8yo Preteen Amy In The Bath And Bedroom"

Length: 5:38

Description: This video depicts a prepubescent minor female approximately seven (7) to nine (9) years of age completely naked in a bathtub exposing her vagina and anus to the camera while rubbing her vagina with her hand. The next scene of the video depicts the same prepubescent minor female lying on a bed completely naked with a blindfold on and performing oral sex on an adult male's erect penis.

c. Video: "\_PTHC\_5yo\_kait\_dad\_extasy\_\_Kathie\_getting\_a\_mouthful\_of\_my\_cum"

Length: :40

Description: This video depicts a prepubescent minor female approximately four (4) to six (6) years of age completely naked performing oral sex on an adult male's erect penis.

31. Your Affiant applied for and received a federal arrest warrant on CHANTHALANGSY for violations of Title 18, United States Code, Sections 2252 and 2252A – Receipt of Child Pornography and Possession of Child Pornography. On March 28, 2017, CHANTHALANGSY was encountered and arrested on the outstanding warrant.

32. On April 4, 2017, continued forensic examinations on CHANTHALANGSY's seized iBuyPower CyborgX computer containing the two hard drives, Kingston 120GB Solid State drive and Hitachi 1TB hard drive revealed approximately ninety-one text (.txt) document

files on the Hitachi 1TB hard drive. TFO Schumacher copied the .txt document files and provided them to your Affiant for review.

33. A thorough review showed the documents are believed to have been created and saved by CHANTHALANGSY due to some of the user names listed for various online memberships and accounts such as: “peng1771” and “Pengja”. There is also a saved document entitled “ups chat.txt” that appears to be a conversation between a United Parcel Service (UPS) customer service representative and the user “Peng”.

34. Your Affiant also located and reviewed numerous saved text documents that relate to the direct sale/distribution of illegal narcotics, exploitation of minors, Bitcoin mining and Bitcoin possession through the use of the Surface Web and Dark Web / Darknet.

35. A text document entitled “bitmainwarranty.txt” contains a message sent to Bitmain Warranty where CHANTHALANGSY inquires about the proper procedures that need to be taken in order to return broken or non-working parts for his Antminer model S9 machine.

36. A text document entitled “coke.txt” contains a description that synthetic cocaine is made up of bath salts with the ingredients Methylenedioxypropylone (MDVP) and Lidocaine.

37. A text document entitled “price habitsincorporated.txt” contains a list of what is believed to be the current going rates for the packaging and sale of illegal narcotics:

1g	40
2g	65
3.5g ball	90
7g 1/4 ounce	155
14g 1/2 ounce	280
28g 1 ounce	500
56g 2 ounce	850
84g 3 ounce	1200
112g 4 ounce	1500
224g 8 ounce	2850

1 lb 16 ounce 4500

38. A text document entitled “weed.txt” contains a description of what is believed to be the current sized amounts for the packaging and sale of illegal narcotics:

“Using the standard for today’s dealings, one quarter ounce is 7 grams, and an ounce is 28 grams. A quarter pound will be 112 grams, and four of those, adding up to a pound, is 448 grams”

39. A text document entitled “zerggprice.txt” contains a list of what appears to be an order form from one of the Dark Web / Darknet illegal narcotics marketplaces along with a follow up message between CHANTHALANGSY and an unknown user:

.5 Grams Crystal Meth Ice Shards \$30

1 Grams Crystal Meth Ice Shards \$50

1.75 Grams Crystal Meth Ice Shards \$60

3.5 Grams Crystal Meth Ice Shards \$100  
ESCROW Order

7 Grams Crystal Meth Ice Shards \$190  
7 Grams Crystal Meth Ice Shards  
ESCROW Order

14 Grams Crystal Meth Ice Shards \$355  
14 Grams Crystal Meth Ice Shards  
ESCROW Order

28 Grams Crystal Meth Ice Shards \$550  
28 Grams Crystal Meth Ice Shards  
ESCROW Order

56 G FIRE METH \*\*FREE EXPRESS\*\* \$840  
56 G FIRE METH \*\*FREE EXPRESS\*\*  
ESCROW Order

112 G (4OZ) FIRE METH \*\*FREE EXPRESS\*\* \$1600  
112 G (4OZ) FIRE METH \*\*FREE EXPRESS\*\*  
ESCROW Order

8OZ FIRE METH\*\*FREE EXPRESS\* \$2800  
8OZ FIRE METH\*\*FREE EXPRESS\*

ESCROW Order

1LB (16OZ) FIRE METH \*\*FREE EXPRESS\*\* \$5000

1LB (16OZ) FIRE METH \*\*FREE EXPRESS\*\*

ESCROW Order

“Hey hows it going? For the half pound it would be 3400 and for the full it would be 6000.....Let me know and I could put up a custom listing..”

40. Your Affiant also located and reviewed numerous text documents entitled “biitcoin”, “bitcoiin”, “bitcoin difficulty history”, “bitcoin forum”, “bitcoin”, “bitcoinn”, “bitsino”, “coinbase”, “miner”, “monero” and “wallett” which contained what is believed to be usernames, passwords and logins for cryptocurrency banks, websites and SUBJECT ACCOUNTS. Within these text documents were the following Bitcoin digital currency wallet numbers:

- 1KXhP8nUtNzjKFGQQXDFubhMQ8LfVdKJ2Y
- NFAUpuGFa2HHygsHTsYZp7rLki89VZb5ye
- MyJFDbxQbNh6jUJVwX9yJL2kaAfcdbd9uwr
- 42DpM2KJjD2HVVAqLqsNpJ2AF9fiw72x9jGEHZA7DtXMYjUgqMYg6D3WbwaVe4vU  
MveKAzAiA4j8xgUi29TpKXpm3y9FQS2
- 17F5rCCPArYwg4pN4amA4naG99D3cCu6F7

41. A text document entitled “torr.txt” contains a link to the Dark Web / Darknet of “http://mt3plrzdiiyqf6jim.onion/renewal/payment.php with a username and password login for the site believed to have been created by CHANTHALANGSY. Your Affiant then conducted authorized undercover operations and gained access to the above referenced TOR site through a fictitiously created user profile. Upon entering the site, your Affiant observed numerous videos entitled and containing child pornography. One of the videos observed by your Affiant was titled “(pthc) 9yo Jenny blows Dad & Dog.mpg”. Screen shots of the video depicted a prepubescent minor female performing oral sex on an adult male’s penis. *Further review of the site showed that users can gain VIP access by making payments through Bitcoin wallets of 0.04*

*for 110 downloads, 0.06 for 230 downloads and 0.08 for six months of unlimited downloads.*

The text file with the Dark Web / Darknet site saved by CHANTHALANGSY containing the terms “renewal/payment” is apparent to your Affiant to be payments made through SUBJECT ACCOUNTS for access to child pornography sites.

42. A text document entitled “torrrr.txt” contains a link to the Dark Web / Darknet of “http://childsplayboq3sq.onion/” with a username and password login for the site believed to have been created by CHANTHALANGSY. Also located within the text document were lists called “cofeebeans pw verschoorloecasains pthccc/girlpa BEcode yw....LostP@ChildsP jam Dune@ChildsPlay”. Your Affiant then conducted authorized undercover operations and gained access to the above referenced TOR site through a fictitiously created user profile. Upon entering the site, your Affiant observed that there were various channels and forums all centralized around child exploitation. Your Affiant then entered a chat room titled “Baby and Infants” and found posts related to child pornography such as “this board is for the posting of images and videos of newborns and infants”. The users in the chat room communicating were listed by their user name @ChildsPlay. Your Affiant believes that the saved lists within the text documents were Dark Web / Darknet users within a child pornography site that CHANTHALANGSY was having conversations with online.

43. A text document entitled “torsite.txt” contains the following list of Dark Web / Darknet sites. Your Affiant then conducted authorized undercover operations and gained access to the below referenced TOR sites through a fictitiously created user profile and described them below.

alphabaywyjrktqn.onion  
stbux7lrtpcgca2.onion  
jsbpbdf6mpw6s2oz.onion  
zdfvqospmrbvzdn3.onion

sszoxp4dqmt24jng.onion  
nracund2vx6lxzck.onion  
lo4wpvx3tcdbqra4.onion

All of the listed sites directed your Affiant to the “AlphaBay Market” which showed to be a marketplace for sale or purchase of illegal narcotics, weapons, fraudulent documents, and hacking tools through SUBJECT ACCOUNTS by CHANTHALANGSY.

44. A text document entitled “ttt.txt” contains the Dark Web / Darknet site “http://pwoah7foa6au2pul.onion/register.php” with a username and password for the site. Your Affiant found that this is one in the same site linked to the “AlphaBay Market” believed to have been utilized by CHANTHALANGSY to purchase illegal narcotics through SUBJECT ACCOUNTS for distribution in the Northwest Arkansas area.

45. Your Affiant is aware that cryptocurrency (Bitcoin) exchangers and Dark Web / Darknet account users must use a computer or other electronic device, such as a smartphone, to conduct transactions with their Bitcoin customers and Dark Web / Darknet associates. The Bitcoin exchangers also must establish electronic wallets to receive and send the Bitcoins during these transactions. These wallets are electronic in nature and may be stored on mobile devices (phones or tablets), external or removable media, and/or computers. Your Affiant is also aware that Bitcoin exchangers and Dark Web / Darknet users can back-up wallets or usernames and passwords to paper printouts that would contain information to restore the wallet or user account in an electronic form. Passwords for access to Bitcoin wallets and Dark Web / Darknet user accounts are typically complex and are often written down or saved in an accessible manner on paper or on some electronic device. Due to the inherent illicit and anonymous nature of these Bitcoin wallets and Dark Web / Darknet accounts there is no identified service provider for these accounts, legitimate, compliant or not, to which legal process may be served, and your Affiant

believes that a seizure warrant served on the owner of the wallets and accounts is the only manner to recover digital currency and investigate further child exploitation contained therein.

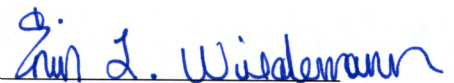
**CONCLUSION**

46. Based on the above facts, your Affiant respectfully asserts there is probable cause that contained within the SUBJECT ACCOUNTS contain digital currency and evidence regarding the purchase or sale of illegal narcotics/child pornography involved in violations of Title 18, United States Code, Sections 2251 and 2252 and Title 21, United States Code, Sections 841.



Gerald Faulkner, Special Agent  
Homeland Security Investigations

Affidavit subscribed and sworn to before me this 17th day of April 2017



Erin L. Wiedemann  
United States Magistrate Judge